# ASDM 6.4: Esempio di configurazione del tunnel VPN da sito a sito con IKEv2

## Sommario



## Introduzione

In questo documento viene descritto come configurare un tunnel VPN da sito a sito tra due appliance Cisco Adaptive Security Appliance (ASA) utilizzando Internet Key Exchange (IKE) versione 2. Viene descritta la procedura utilizzata per configurare il tunnel VPN con una GUI guidata di Adaptive Security Device Manager (ASDM).

## Prerequisiti

### Requisiti

Verificare che Cisco ASA sia stato configurato con le impostazioni di base.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASA serie 5500 Adaptive Security Appliance con software versione 8.4 e successive
- Software Cisco ASDM versione 6.4 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

### Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

## Premesse

IKEv2 è un miglioramento del protocollo IKEv1 esistente che include i seguenti vantaggi:

- Meno scambi di messaggi tra peer IKE
- Metodi di autenticazione unidirezionale
- Supporto integrato per Dead Peer Detection (DPD) e NAT-Traversal
- Utilizzo del protocollo EAP (Extensible Authentication Protocol) per l'autenticazione
- Eliminazione del rischio di attacchi DoS semplici mediante l'utilizzo di cookie anti-clogging

## Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

**Nota: per** ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

### Esempio di rete

Nel documento viene usata questa impostazione di rete:


In questo documento viene illustrata la configurazione del tunnel VPN da sito a sito su HQ-ASA. La stessa operazione può essere eseguita anche come mirror sull'appliance BQ-ASA.

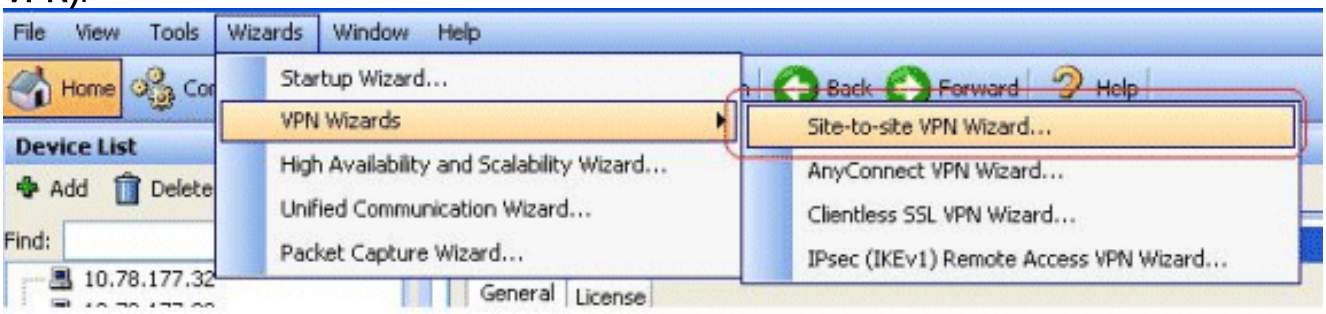
### Configurazione ASDM su HQ-ASA

Questo tunnel VPN può essere configurato usando una semplice procedura guidata GUI.

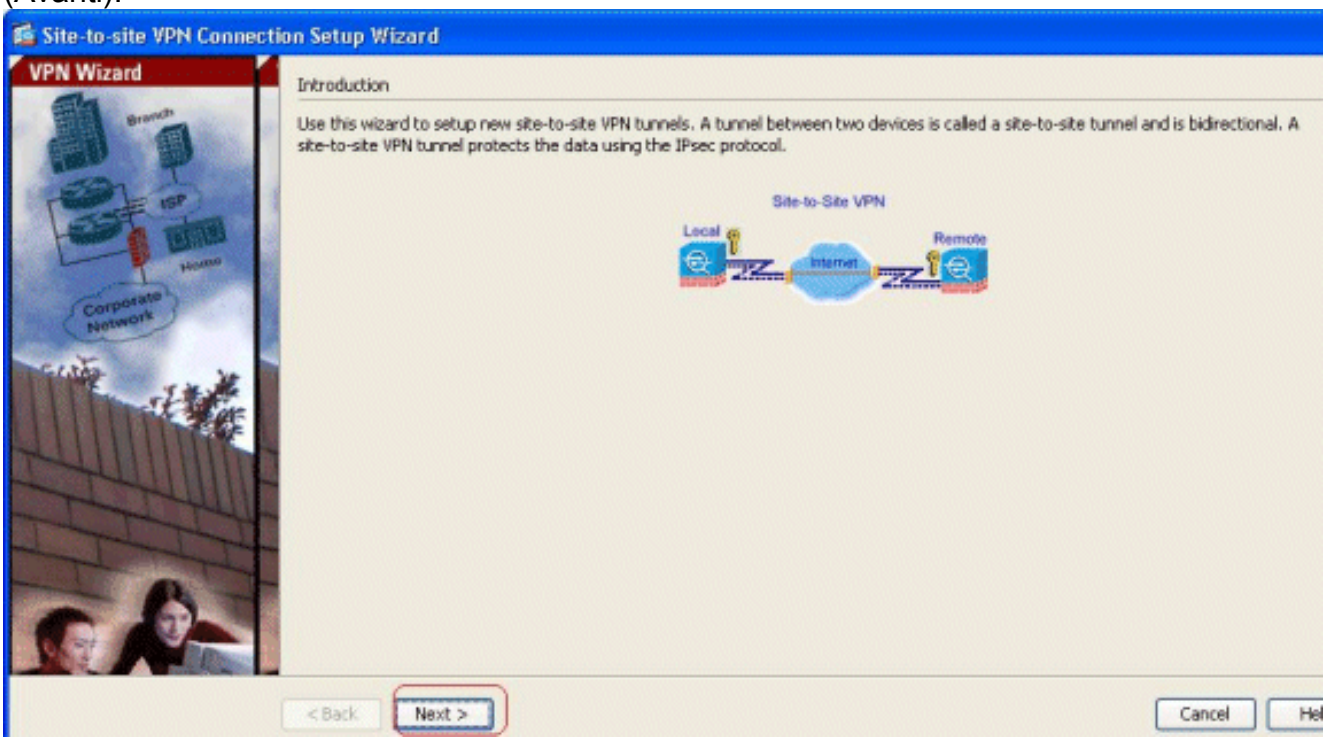
Attenersi alla seguente procedura:

1. Accedere ad ASDM e selezionare **Wizards > VPN Wizard > Site-to-site VPN Wizard** (Procedure guidate

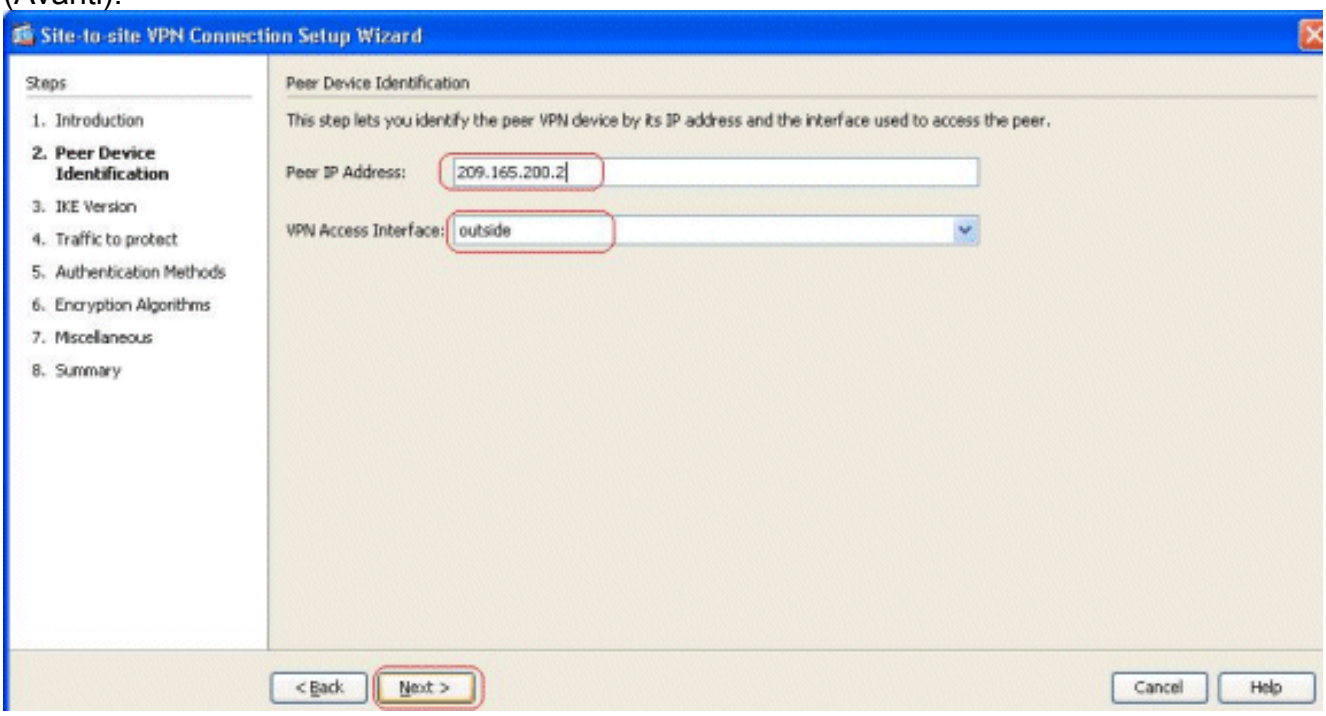
VPN).



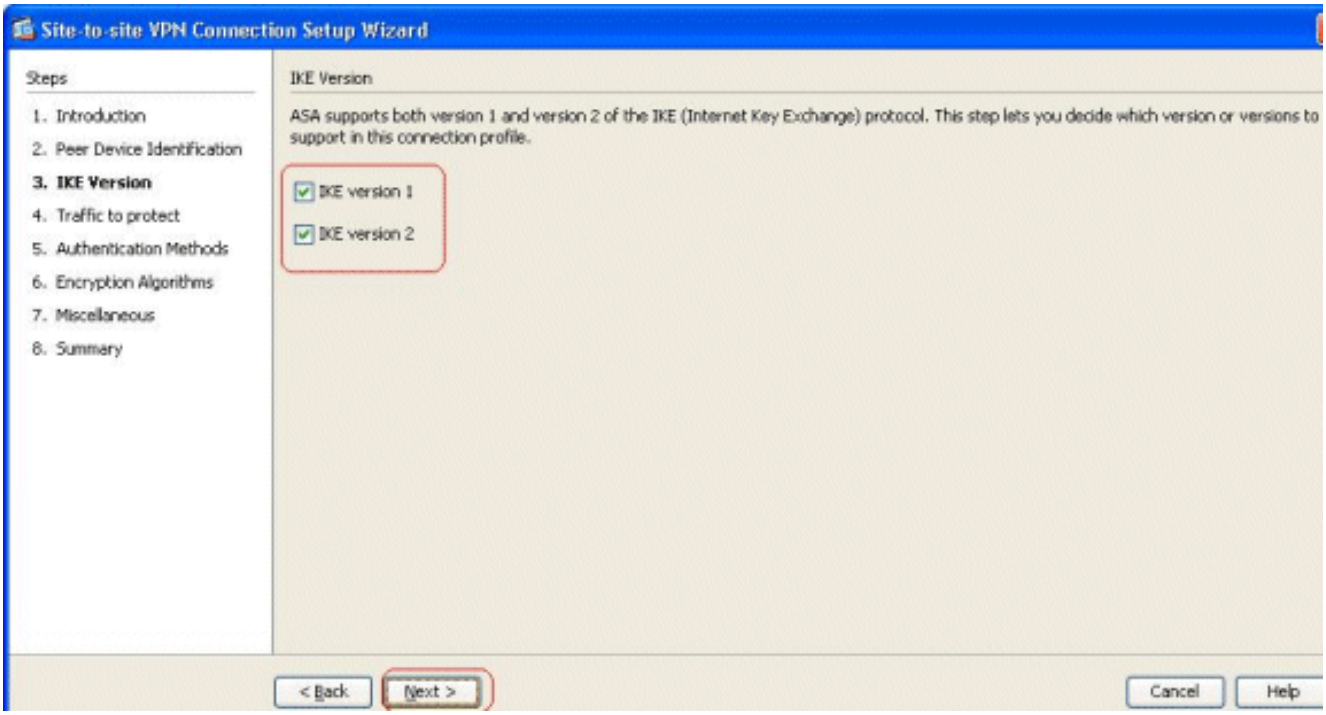

2. Viene visualizzata una finestra di impostazione della connessione VPN da sito a sito. Fare clic su **Next**
(Avanti).




3. Specificare l'indirizzo IP peer e l'interfaccia di accesso VPN. Fare clic su **Next**
(Avanti).

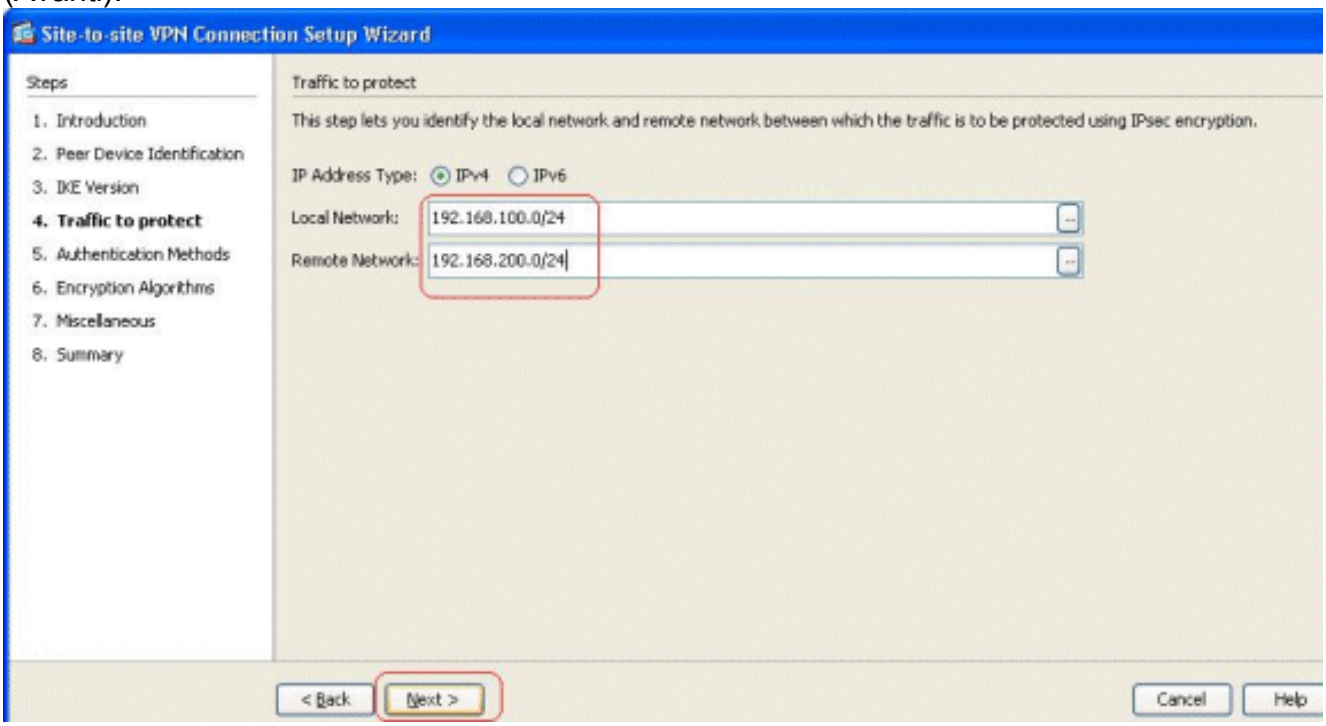


4. Selezionare entrambe le versioni IKE e fare clic su **Avanti**.

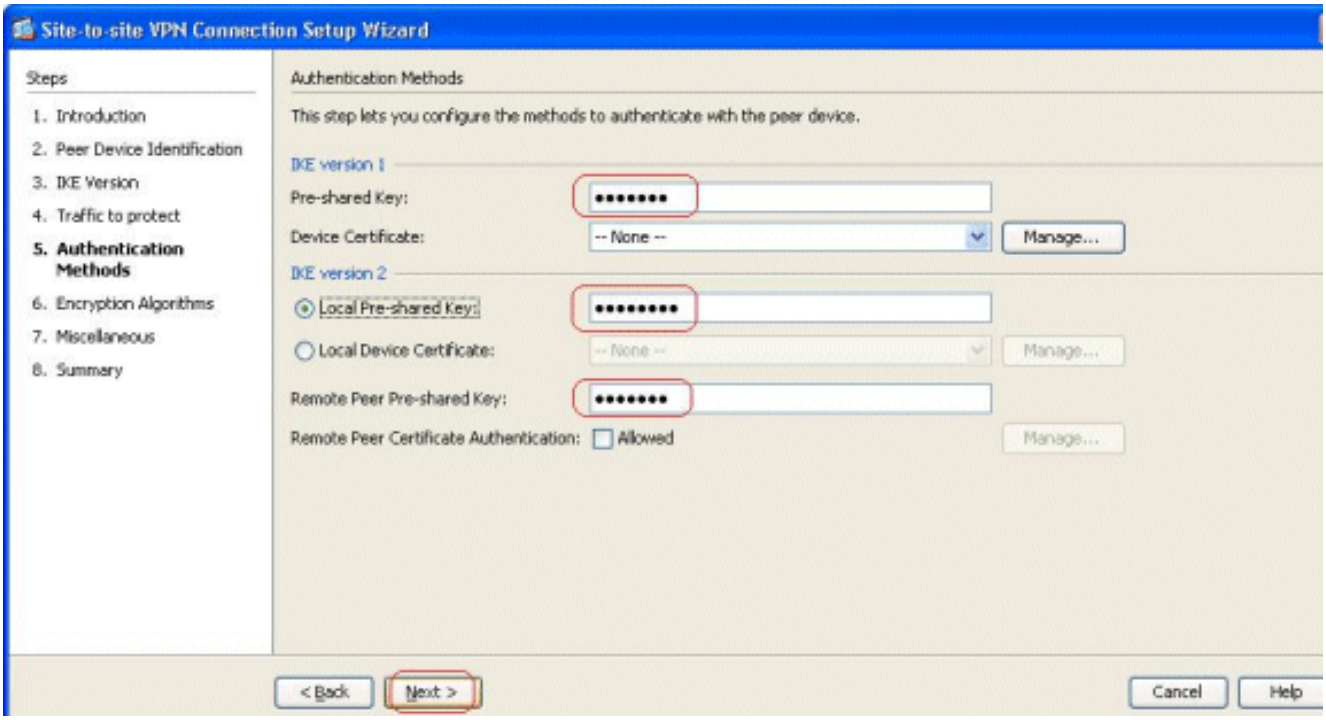



**Nota:** entrambe le versioni di IKE sono configurate qui perché l'iniziatore potrebbe avere un backup da IKEv2 a IKEv1 quando si verifica un errore di IKEv2.

5. Specificare la rete locale e la rete remota in modo che il traffico tra queste reti venga crittografato e passato attraverso il tunnel VPN. Fare clic su **Next** (Avanti).

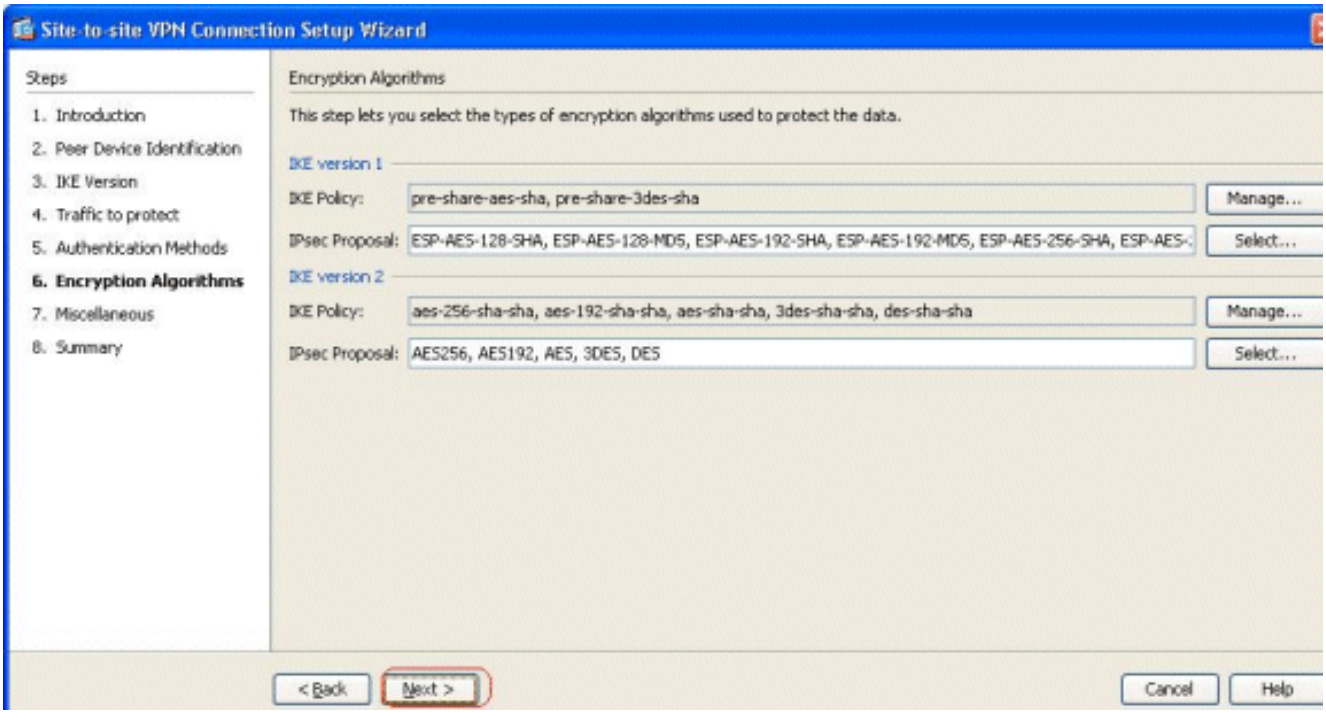



6. Specificare le chiavi già condivise per entrambe le versioni di IKE.

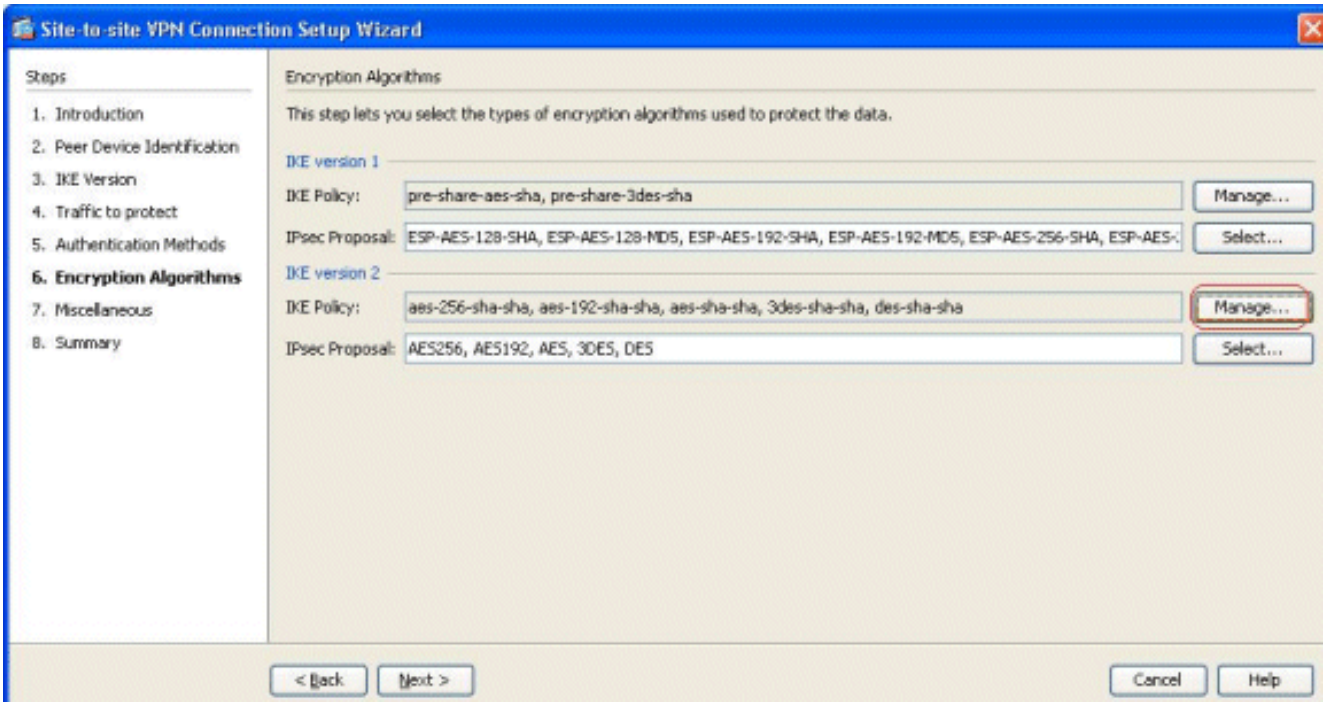



La differenza principale tra IKE versioni 1 e 2 consiste nel metodo di autenticazione consentito. IKEv1 consente un solo tipo di autenticazione a entrambi i terminali della VPN (chiave precondivisa o certificato). Tuttavia, IKEv2 consente di configurare i metodi di autenticazione asimmetrica (ovvero l'autenticazione con chiave precondivisa per il mittente, ma l'autenticazione del certificato per il risponditore) utilizzando CLI di autenticazione locale e remota separate.Inoltre, è possibile avere diverse chiavi già condivise su entrambe le estremità. La chiave locale pre-condivisa all'estremità HQ-ASA diventa la chiave remota pre-condivisa all'estremità BQ-ASA. Analogamente, la chiave remota pre-condivisa sull'estremità HQ-ASA diventa la chiave locale pre-condivisa sull'estremità BQ-ASA.

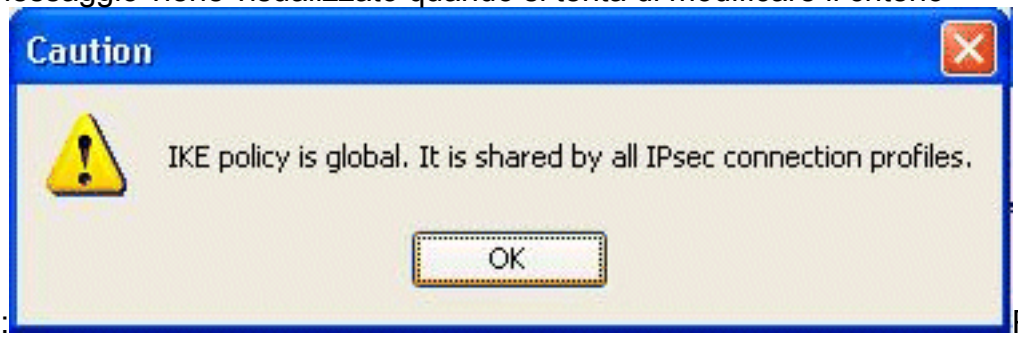
7. Specificare gli algoritmi di crittografia per IKE versioni 1 e 2. I valori predefiniti sono accettati:



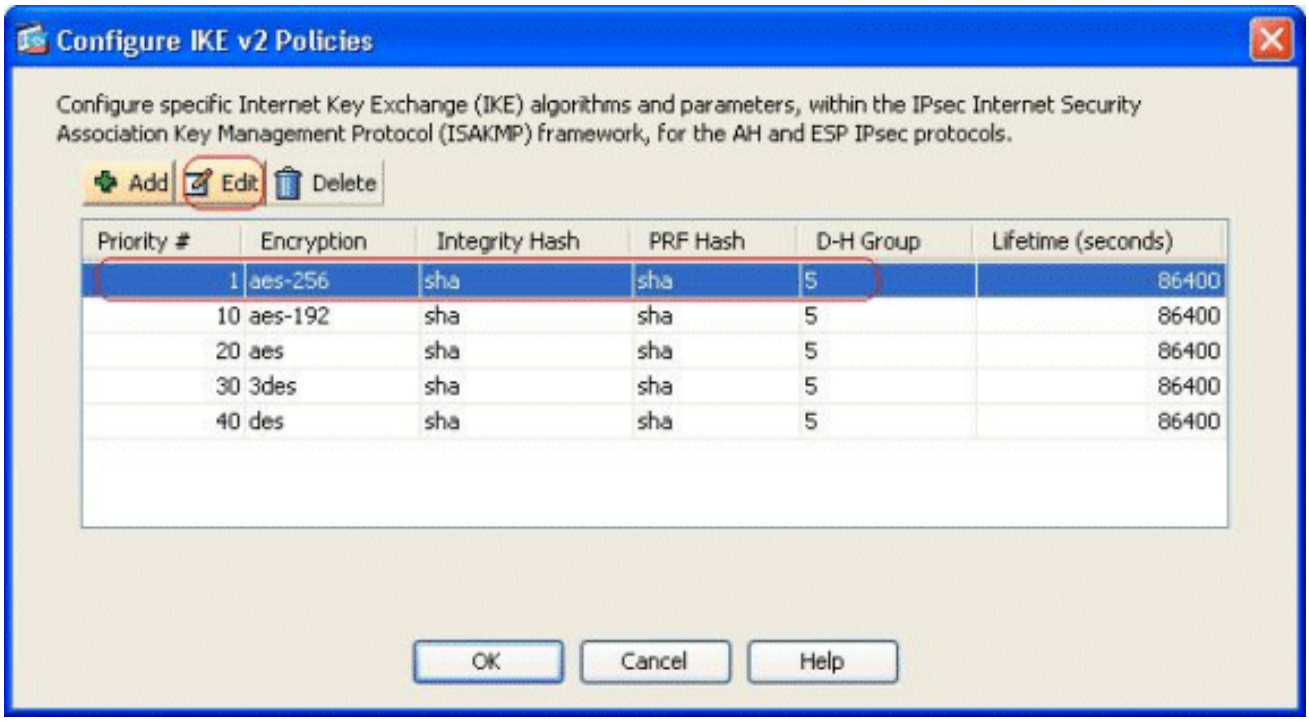

8. Per modificare il criterio IKE, fare clic su **Gestisci**...




**Nota: Il criterio IKE** in IKEv2 è sinonimo del **criterio ISAKMP** in IKEv1.**Proposta IPSec** in IKEv2 è sinonimo di **Trasformazione impostata** in IKEv1.

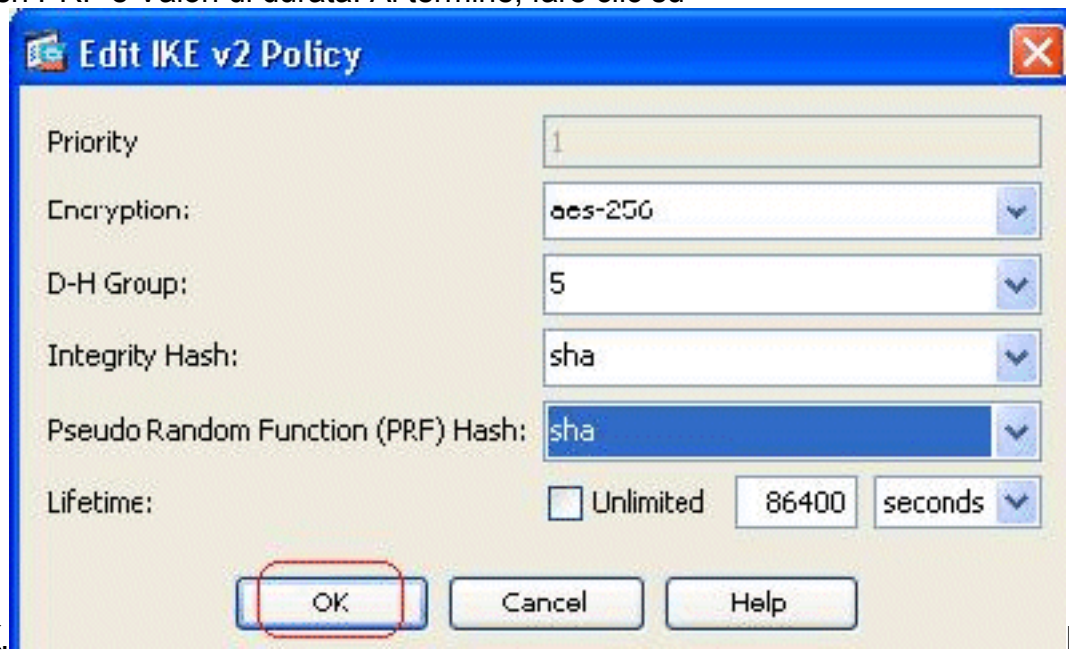
9. Questo messaggio viene visualizzato quando si tenta di modificare il criterio esistente: 

Per continuare, fare clic su **OK**.
10. Selezionare il criterio IKE specificato e fare clic su **Modifica**.



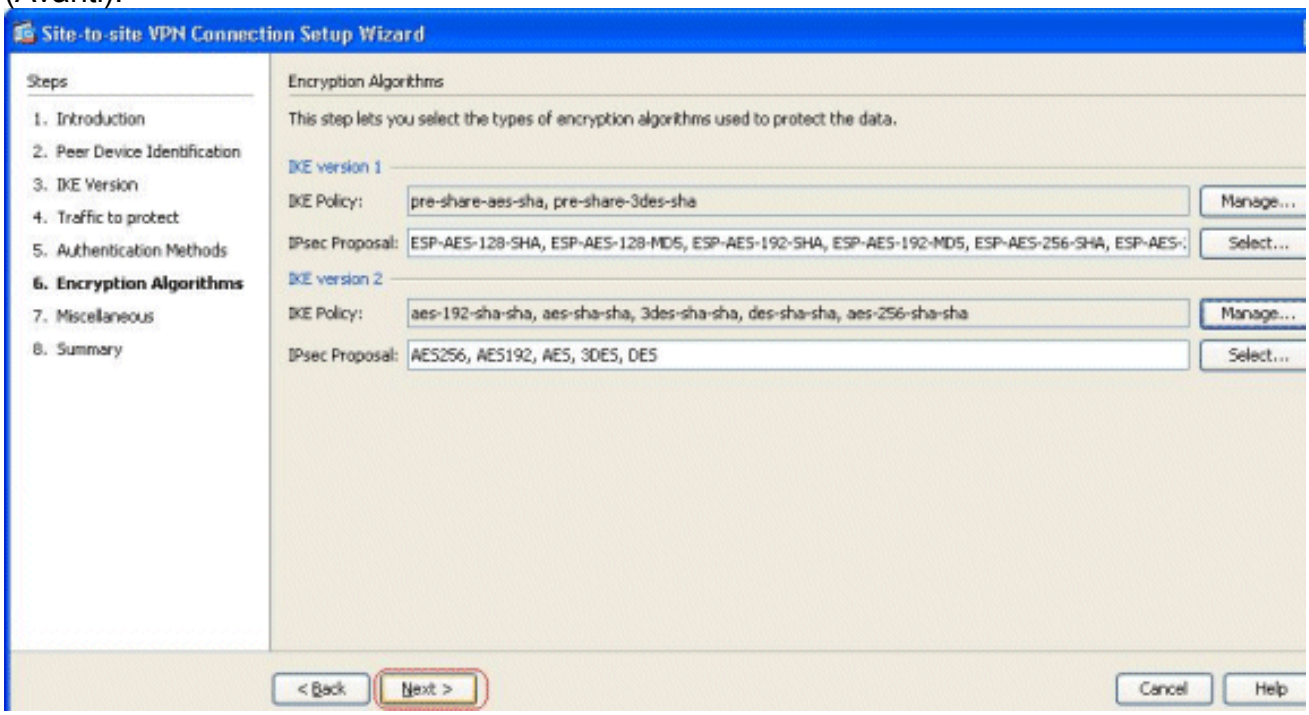

11. Èpossibile modificare parametri quali Priorità, Crittografia, Gruppo D-H, Hash di integrità,

Hash PRF e Valori di durata. Al termine, fare clic su

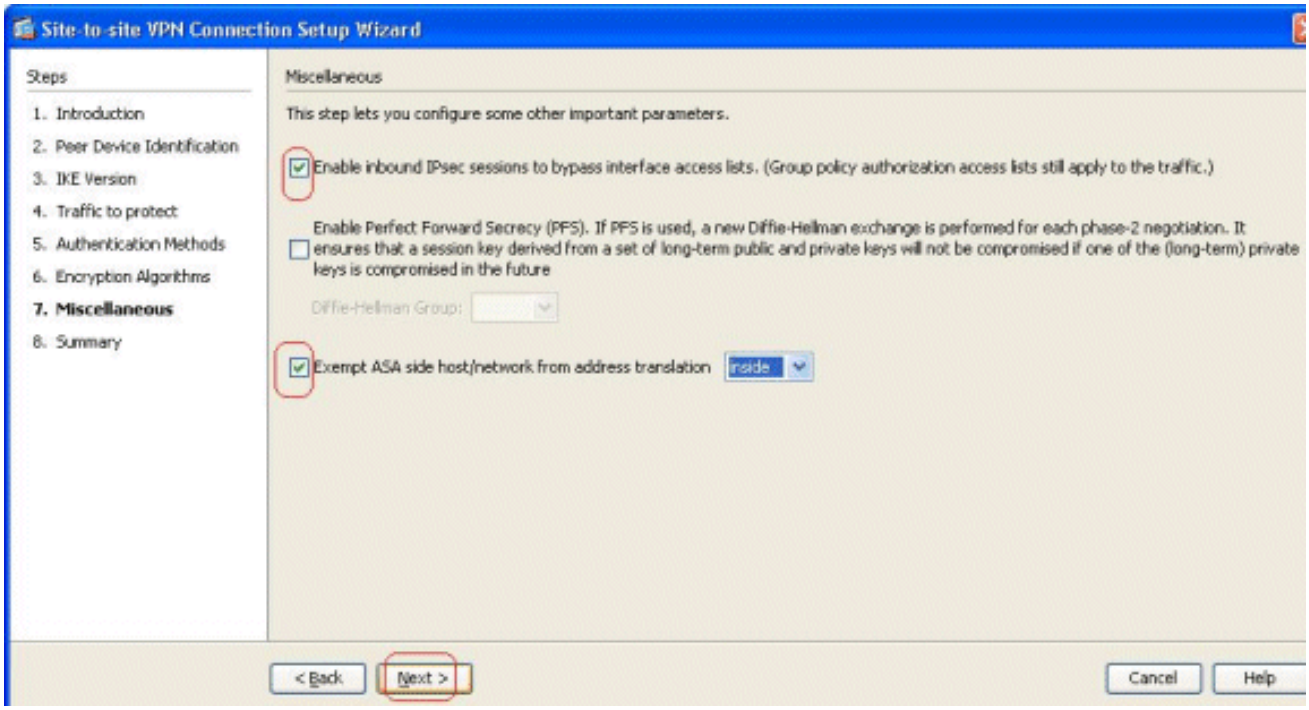



**OK**. IKEv2 consente di negoziare l'algoritmo Integrity separatamente dall'algoritmo PRF (Pseudo Random Function). È possibile configurare questa opzione nel criterio IKE con le opzioni disponibili correnti SHA-1 o MD5.Non è possibile modificare i parametri della proposta IPSec definiti per impostazione predefinita. Per aggiungere nuovi parametri, fare clic su **Select** (Seleziona) accanto al campo IPsec Project (Proposta IPSec). La differenza principale tra IKEv1 e IKEv2, in termini di proposte IPsec, è che IKEv1 accetta la trasformazione impostata in termini di combinazioni di algoritmi di crittografia e autenticazione. IKEv2 accetta i parametri di crittografia e integrità singolarmente e rende infine possibili tutte le combinazioni di parametri OR. È possibile visualizzarli al termine della procedura guidata nella diapositiva Riepilogo.

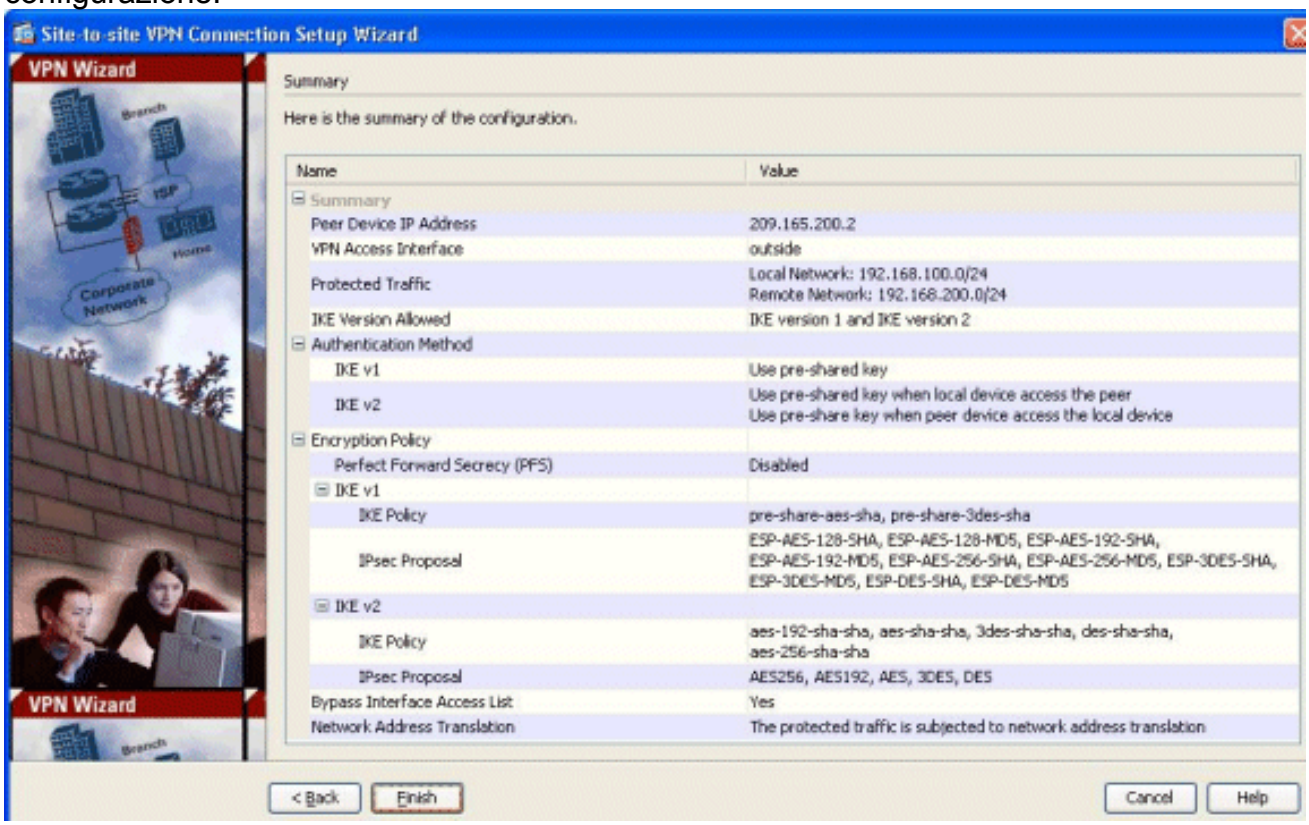
12. Fare clic su **Next** (Avanti).




13. Specificare i dettagli, ad esempio l'esenzione NAT, PFS e il bypass dell'ACL di interfaccia. Scegliere **Successivo**.




14. Di seguito è riportato un riepilogo della configurazione:




Per completare la procedura guidata del tunnel VPN da sito a sito, fare clic su **Fine**. Viene creato un nuovo profilo di connessione con i parametri configurati.

## Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- show crypto ikev2 sa: visualizza il database SA di runtime IKEv2.
- show vpn-sessiondb detail l2l: visualizza le informazioni sulle sessioni VPN da sito a sito.

# Risoluzione dei problemi

## Comandi per la risoluzione dei problemi

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

**Nota:** consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- debug crypto ikev2: visualizza i messaggi di **debug** per IKEv2.

# Informazioni correlate

- Appliance Cisco ASA serie 5500 - Supporto tecnico
- Documentazione e supporto tecnico – Cisco Systems